DEC 4 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE (COMPTROLLER/CHIEF
FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
GENERAL COUNCIL

Subject: Promulgation of DOD Policy For Assessment, Test, and Evaluation of Information Technology System Interoperability

By this letter, we the undersigned promulgate DOD Policy For Assessment, Test, and Evaluation of Information Technology System Interoperability.

The purpose of this policy is to identify interoperability problems in information technology (IT) systems (in development, in production, or deployed) and to oversee any corrective actions that are necessary. To minimize additional workloads both for our staffs and for affected Program Managers (PMs) this policy creates two levels of review below formal Test and Evaluation (T&E) Oversight: a Watch List and a Review List.

- At the discretion of the four signatories, programs deemed to have significant interoperability deficiencies will be placed on an Interoperability Watch List.
- The Interoperability Review List contains programs with interoperability problems which we consider less critical or for which the PM is making good progress in resolving.

Programs on both lists will be reviewed periodically by our staffs and, at our discretion, either retained in their present status, moved to a different list, or proposed for formal T&E oversight.

Jacques S. Gansler 02 OCT 2000
Under Secretary of Defense
Acquisition, Technology, and Logistics

Philip E. Coyle
Director 22 SEP 2000
Operational Test and Evaluation

Arthur L. Money
Assistant Secretary of Defense
Command, Control, Communications, and
Intelligence DEC 4 2000

S. A. Fry
Vice Admiral, U.S. Navy
Director, Joint Staff

POLICY FOR ASSESSMENT, TEST, AND EVALUATION OF INFORMATION TECHNOLOGY SYSTEMS INTEROPERABILITY

This document establishes the process to address deficiencies in the interoperability of information technology (IT) systems[1] and to oversee any corrective actions that are necessary. Subsequent guidance for implementing this policy will be established by senior officials from the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics [USD(AT&L)]; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/DoD Chief Information Officer [ASD(C3I)/DoD CIO]; the Director of the Joint Staff; and the Director, Operational Test and Evaluation (DOT&E). These offices, hereafter referred to as the four signatories to this policy, will promote and enforce DoD processes to ensure that IT systems are properly evaluated for technical and operational interoperability.[2] The policy described in this document will be migrated into the next revisions of the DoD 5000 series regulations, DoD Directive (DoDD) 4630.5, and DoD Instruction (DoDI) 4630.8, and will be reviewed at the one-year anniversary to ensure it is value-added and optimally effective.

BACKGROUND

Information superiority is a key tenet of Joint Vision 2020. A necessary condition to attain information superiority is for IT systems to exchange and use information in a timely manner and operate together effectively. Effective interoperability depends on the recognition that interoperability is about interdependencies and interfaces between and among systems (i.e., it is about families-of-systems or systems-of-systems) in a mission-area context. Attainment of information superiority also requires adequate information assurance.[3]

Title 10 designates the DoD CIO as responsible for ensuring the interoperability of IT and National Security Systems throughout the DoD, and makes Military Department CIOs responsible for ensuring that IT systems are interoperable with other relevant IT

[1] For purposes of this policy memorandum, information technology systems are systems based on information technology and include National Security Systems (NSSs) referred to in the Clinger-Cohen Act of 1996 as telecommunications or information parts of weapons or weapon systems, command, control, communication, computer, intelligence, surveillance and reconnaissance (C4ISR) systems; automated information systems, and certain critical information systems. See definitions in the appendix.

[2] The process established in this policy memorandum and developed in subsequent guidance will be in accordance with the Department's Integrated Product and Process Development concept defined in DoD Regulation 5000.2-R.

[3] See DOT&E Policy Memorandum, "Policy for Operational Test and Evaluation of Information Assurance," November 17, 1999.

systems of the government and the DoD.[4] Further, two goals outlined by the USD(AT&L) concerning interoperability are 1) to achieve interoperable, integrated, and secure command, control, communications, computer, and intelligence (C4I), and 2) to achieve not only joint (inter-Service) interoperability, but also combined and coalition partner interoperability.[5]

Interoperability definition, policy formulation, and policy implementation are prescribed in Joint Chiefs of Staff Publication 1-02, FED-STD-1037C, DoD Regulation 5000.2-R, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, DoDD 4630.5, DoDI 4630.8, and CJCSI 6212.01B.

Despite the long-standing existence of DoD policy on interoperability and a process for interoperability certification, interoperability problems with IT systems persist. A report on the 1999 Operation Allied Force (Kosovo) cited numerous combined-interoperability problems.[6] A 1998 General Accounting Office (GAO) report identified weaknesses in the DoD's interoperability certification process.[7] The Commanders-in-Chief (CINCs) of the Unified Commands have frequently raised interoperability issues via the Joint Staff's Joint Warfighting Capability Assessment (JWCA) process, the CINC Interoperability Program Offices (CIPOs), and other fora. This policy responds to these concerns by addressing oversight of interoperability development of IT systems.

APPLICABILITY AND SCOPE

This policy applies to all DoD Major Defense Acquisition Programs, programs on the Test and Evaluation Oversight list, post-acquisition (legacy) systems, and all programs and systems that must interoperate with them (e.g., pre-acquisition demonstrations [Advanced concept Technology Demonstrations (ACTDs) and Joint Warrior Interoperability Demonstration (JWID) Golden Nuggets that lead to acquisitions], and non-5000 series acquisitions [e.g., CINC Initiative Programs]). This policy covers intra-Service, inter-Service, and combined and coalition interoperability between and among IT systems that exchange and use information to enable systems, units, or forces to operate effectively together. Interoperability in this policy refers to both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

[4] Title 10 United States Code, Section 2223 (Public Law 105-261, Strom Thurmond National Defense Authorization Act for FY 1999, Sec. 331).

[5] Remarks by the Hon. Jacques S. Gansler, Under Secretary of Defense (Acquisition, Technology, and Logistics), to the AIAA Executive Forum, Washington, DC, January 28, 1999.

[6] Kosovo/Operation Allied Force, report in draft as of December1999.

[7] "Joint Military Operations, Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability," GAO/NSIAD 98-73, General Accounting Office, March 1998.

DEFINITIONS

Terms used in this policy are defined in the appendix.

PROCEDURES

DoD policy for the interoperability of IT systems will be enforced by the four signatories to this policy through the establishment of the Interoperability Watch List. At the discretion of the four signatories, programs and systems deemed to have significant interoperability deficiencies will be placed on the Interoperability Watch List. Program Managers or Cognizant Officials (PMs/COs) for a program or system on the Watch List will be required to undertake corrective actions to address interoperability deficiencies in order to be removed from the Interoperability Watch List. If the deficiencies persist, the program or system may be recommended for the T&E Oversight List.

The procedure associated with the Interoperability Watch List is illustrated in Figure 1. The procedure consists of two parts: a program and system interoperability review to decide which programs or systems are to be added to the Interoperability Watch List, and an assessment of programs and systems on the Interoperability Watch List to determine if interoperability deficiencies are being adequately addressed. To the maximum extent possible, existing fora (e.g., the MCEB, the CIO Executive Board, etc.) will be employed, as appropriate, to accomplish the Watch List review.

Program and System Interoperability Review

Any DoD organization may identify to the four signatories programs and systems with interoperability deficiencies, and recommend they be considered for the Interoperability Watch List. Likely sources are: 1) the offices of the four signatories, 2) the Operational Test Agencies (OTAs), 3) the CINCs of the Combatant Commands (via the JWCA process and the CIPOs), 4) program management offices, 5) the Military Communications-Electronics Board (MCEB) (via the Interoperability Policy and Testing Panel), 6) the Military Intelligence Board (MIB), 7) the Defense Information Systems Agency (DISA), and 8) the Joint C4ISR Battle Center.

Staff members of the four signatories will review existing documentation and performance results associated with those programs and systems recommended for Interoperability Watch, and on a quarterly basis will develop an Interoperability Review List. Once a program or system has been placed on the Review List, the PM/CO will be notified and invited to provide additional or clarifying information. From the Interoperability Review List, a subset with the most critical deficiencies will be nominated for review by senior representatives of the four signatories. While on the Review List, the PM/CO will not be required to create any additional documentation for the four signatories.

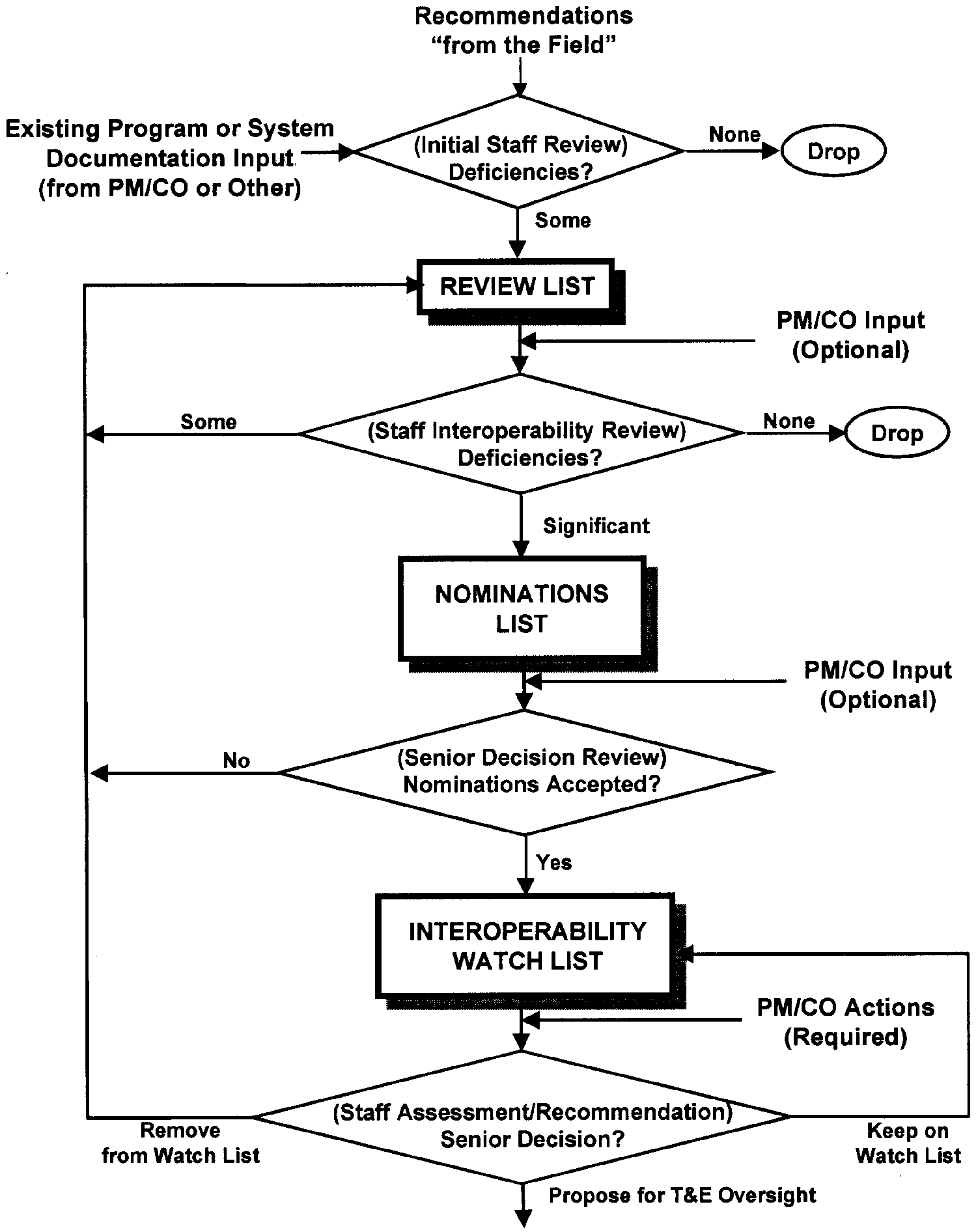
Recommendations "from the Field"
Existing Program or System Documentation Input (from PM/CO or Other)
(Initial Staff Review) Deficiencies?
None
Drop
Some
REVIEW LIST
PM/CO Input (Optional)
Some
(Staff Interoperability Review) Deficiencies?
None
Drop
Significant
NOMINATIONS LIST
PM/CO Input (Optional)
No
(Senior Decision Review) Nominations Accepted?
Yes
INTEROPERABILITY WATCH LIST
PM/CO Actions (Required)
(Staff Assessment/Recommendation) Senior Decision?
Remove from Watch List
Keep on Watch List
Propose for T&E Oversight

Figure 1. Process for Interoperability Review and Assessment

Approximately thirty days after the nomination list is finalized, the senior-level selection review will be convened, as necessary, with PM/COs of nominated programs and systems invited to attend. Those programs and systems for which interoperability is deemed to be critical, and insufficient evidence exists that interoperability issues are being addressed, will be selected for the Interoperability Watch List to ensure that appropriate attention is given to achieving interoperability objectives. Notification of selection for the Interoperability Watch List will be provided to the PM/CO by formal memorandum that identifies shortfalls and required actions; one likely action may involve development of an Interoperability Improvement Plan, which will incorporate appropriate elements of the seven-step process for systems on T&E Oversight (see below). Those programs and systems that are not selected for the Watch List will be retained on the Review List for the next review cycle, and until such time as the staff-level review determines there are no interoperability deficiencies of significance. The Interoperability Watch List will be updated and published quarterly.

Programs and Systems under Interoperability Watch

Programs and systems on the Interoperability Watch List will provide periodic updates of current status towards correcting identified deficiencies to the offices of the four signatories. These updates will be provided by the PM/CO and the responsible test organization (either developmental or operational), in conjunction with the Joint Interoperability Test Command (JITC). These updates will support an assessment[8] by staff members of the four signatories, who will advise the senior-level review whether interoperability issues are being adequately addressed, and whether a status change is warranted (i.e., whether the program or system should be removed from the Interoperability Watch List, kept on the Interoperability Watch List, or proposed for T&E Oversight). Quarterly reports summarizing the activities of systems and programs on the Watch List will be prepared by staff members of the four signatories.

Programs on T&E Oversight

The following seven-step process provides a comprehensive methodology for assessing interoperability, and will be specifically applied to programs on the T&E Oversight List. Elements of this process may also be applied to programs and systems on the Interoperability Watch List, as appropriate for the development and execution of an Interoperability Improvement Plan.

(1) Requirements and Test Documentation: The TEMPs and operational test plans must include at least one critical technical parameter and one operational effectiveness issue for the evaluation of interoperability. These documents should also specify interoperability test concepts. The TEMPs should reference and extract requirements from the appropriate MNSs, CRDs, ORDs, C4ISPs, and integrated architectures. The Joint Staff will ensure that all MNSs, CRDs, and ORDs contain specific, testable, and measurable interoperability requirements and key performance parameters (KPPs) as

[8] This assessment will be coordinated with the interoperability certification process (see definition in the appendix) as prescribed in CJCSI 6212.01B.

specified in CJCSI 3170.01A. USD(AT&L) and ASD(C3I)/DoD CIO will ensure that C4ISPs and integrated architectures reflect the appropriate family-of-systems context to support the systems interoperability requirements. The OTAs, the Joint Staff, and the system user or program proponent, in conjunction with DISA/JITC, should develop the test procedures and effectiveness measures based on the requirements and expected concepts of operations for the systems. The OTAs may develop additional issues to add to the TEMP and test plans based on the DoD 5000 series regulations for interoperability.

(2) Developmental Testing: An objective of Developmental Testing (DT) is to reduce program risk by providing early identification of technical interoperability problems. The emphasis of both contractor and Government DT is to determine whether specific technical information exchange requirements (e.g., standards, protocols, and interface controls) have been adequately demonstrated prior to entering formal operational testing. Interoperability results from DT will be assessed during Operational Test Readiness Reviews.

(3) Operational Assessments (OAs): An objective of OAs is to reduce program risk by providing early identification of potential problems. A system-level assessment of the viability of plans and resources to test and evaluate interoperability should be conducted for the system at Milestone I or at the System Integration Milestone, whichever comes first, and at subsequent milestones. Such OAs should leverage the Preliminary/Critical Design Reviews, developmental testing, and other appropriate sources (e.g., information assurance testing) to produce operational interoperability assessments.

(4) Operational Test Readiness Reviews (OTRRs): All available interoperability assessments (e.g., OAs, JITC compatibility and interoperability assessments) should be reviewed during the OTRR before conducting Initial OT&E. Potentially critical interoperability problems must be highlighted for assessment during OT&E.

(5) Operational Testing: As part of the OT&E, the OTAs will include interoperability evaluations. These evaluations will assess the adequacy of interoperability in the accomplishment of the mission for the proposed system within the context of the system's intra-Service, inter-Service (joint), and combined/coalition expected operational environment. Operational test plans will be written to include the operational interoperability evaluation and supporting measures for the critical operational effectiveness issues. Interoperability measures will be focused on both the ability of the subject system to exchange information and services accurately and in a timely manner, and the effect of interoperability problems on mission accomplishment. DOT&E and the OTAs will develop guidelines to assist in the evaluation of overall operational interoperability capabilities.

(6) Certification Testing: : All National Security Systems (NSS) and IT systems, regardless of ACAT, must be tested and testing results certified by DISA (JITC). Testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early user test) whenever possible to conserve resources. Interoperability evaluation and testing will be conducted throughout the life cycle of NSS and IT systems and interfaces, but should be achieved as early as is practical to support scheduled procurement decisions. The J-6 validates that the interoperability KPP derived from the set of top-level information exchange requirements (IERs) approved in the CRD (if applicable), ORD, and C4ISP was adequately tested and testing results certified during the DISA (JITC) interoperability system test certification.

(7) Reports: DOT&E will report operational effectiveness in the DOT&E Annual Report and in the Beyond Low-Rate Initial Production reports to the Secretary of Defense and the Congress.

EFFECTIVE DATE

This policy is effective immediately.

Jacques S. Gansler
Under Secretary of Defense
Acquisition, Technology, and Logistics

Philip E. Coyle
Director 22 SEP 2000
Operational Test and Evaluation

19 SEP 2000
Arthur L. Money
Assistant Secretary of Defense/DoD CIO
Command, Control, Communications, and
Intelligence

S. A. Fry
Vice Admiral, U.S. Navy
Director, Joint Staff

APPENDIX: DEFINITIONS

1. C4I System: Any system featuring all or a subset of the following: communications, automated information, or intelligence systems or equipment that assist the commander in planning, directing, and controlling forces. C4I systems consist of hardware, software, personnel, facilities, and procedures and represent the integration of information (including data), information processing, and information transfer systems organized to collect, produce, store, display, and disseminate information. (CJCSI 6212.01B)

2. Certification: The process by which DoD systems with C4I capabilities are evaluated for satisfaction of requirements for interoperability, compatibility, and integration. This process occurs at four levels:

(a) J-6 Interoperability Requirements Certification: The Joint Staff J-6 certifies MNSs, CRDs, and ORDs, regardless of ACAT level, for conformance with joint National Security System (NSS) and information technology system (ITS) policy, doctrine, and interoperability standards. The J-6 also certifies the interoperability key performance parameter (KPP) derived from a set of top-level information exchange requirements (IERs). As part of the review process, J-6 requests assessments from the Services, Defense Information Systems Agency (DISA), and DoD agencies. (CJCSI 6212.01B)

(b) J-6 Supportability Certification: The J-6 certifies to ASD(C3I)/DoD CIO that C4ISPs, regardless of ACAT, adequately address NSS and ITS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems. As part of the review process, J-6 requests supportability assessments from DISA and DoD agencies. (CJCSI 6212.01B)

(c) DISA (JITC) Interoperability Testing and Test Certification: All NSS and ITS, regardless of ACAT, must be tested and testing results certified by DISA (JITC). Testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early user test) whenever possible to conserve resources. Interoperability evaluation and testing will be conducted throughout the life cycle of NSS and ITS and interfaces. (CJCSI 6212.01B)

(d) J-6 Interoperability System Validation: The J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements. The J-6 validates that the interoperability KPP derived from the set of top-level IERs approved in the CRD (if applicable), ORD, and C4ISP was adequately tested and testing results certified during the DISA (JITC) interoperability system test certification. (CJCSI 6212.01B)

3. Information Assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for

restoration of information systems by incorporating protection, detection, and reaction capabilities. (Joint Publication 3-13)

4. Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Vision 2010)

5. Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Joint Pub 1-02)

6. Information Technology: Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. (40 USC 1401 and ITMRA of 1996, Sec 5002)

7. Interoperability:

(a) The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (Joint Pub 1-02)

(b) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (Joint Pub 1-02)

(c) The ability to exchange data in a prescribed manner and the processing of such data to extract intelligible information that can be used to control/coordinate operations. (FED-STD-1037C)

8. Key Performance Parameter (KPP):

Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the Joint Requirements Oversight Council (JROC). ORD KPPs are included in the Acquisition Program Baseline (APB).

9. National Security System (NSS): Any telecommunications or information system operated by the United States Government, the function, operation, or use of which—

(a) involves intelligence activities;

(b) involves cryptologic activities related to national security;

(c) involves command and control of military forces;

(d) involves equipment that is an integral part of a weapon or weapons system; or

(e) subject to limitation below, is critical to the direct fulfillment of military or intelligence missions.

Limitation: Item (e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (40 USC Sec 1452; ITMRA of 1996, Sec 5142)

10. Operational Interoperability: The operational ability (effectiveness and suitability) of systems, units, or forces to provide services/information to and accept services/information from other systems, units, or forces and to use the services/information so exchanged to enable the systems, units, or forces to operate effectively together, under realistic combat conditions, by typical military users employing the necessary tactics, techniques and procedures (or concepts of operations). (Derived from Institute for Defense Analyses Paper P-2229, "Interim Guidelines for Improving Operational Interoperability of Tactical Command, Control, and Communications Systems," 30 August 1989)